ELECTRONIC MAIL SYSTEM WITH AUTHENTICATION/ENCRYPTION METHODOLOGY FOR ALLOWING CONNECTIONS TO/FROM A MESSAGE TRANSFER AGENT

Sub a1

ABSTRACT OF THE DISCLOSURE

~~An electronic mail ("e-mail") system is described that provides methodology~~ to enforce authentication or encryption to/from Mail Transfer Agents and from Mail User Agents. In accordance with the present invention, support is added to enforce certain restrictions on the connections between two hosts (a server and a client), depending on whether sendmail (i.e., Sendmail Message Transfer Agent) acts as a server (receiving e-mail) or as a client (sending e-mail). For instance, in one embodiment of the method, a client's request is received at a message transfer agent (MTA) for establishing a secured connection with the MTA for sending an e-mail message. The method attempts to authenticate the client, through use of a certificate. If the client cannot be authenticated, the method terminates without establishing the secured connection and without sending the e-mail message. On the other hand, if the client can be authenticated, the method establishes the secured connection between the client and the MTA. Additionally, the method (optionally) determines whether the encryption employed for the secured connection meets a predefined minimum encryption strength. If the encryption employed does not meet the predefined minimum encryption strength, the method terminates (including terminating the secured connection without sending the e-mail message). However, if the encryption employed does meet the predefined minimum encryption strength, the MTA will send the e-mail message (for ultimate delivery at a target destination). In this manner, it is possible for each type of connection to enforce an authentication of the other side and/or at least a certain key length of ~~the symmetric cipher used for encryption~~.